UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/666,804	09/21/2000	Douglas E. Trent	P56103C	8933

8439	7590	03/08/2006

ROBERT E. BUSHNELL
1522 K STREET NW
SUITE 300
WASHINGTON, DC 20005-1202

EXAMINER
BANGACHON, WILLIAM L

ART UNIT	PAPER NUMBER
2635	

DATE MAILED: 03/08/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/666,804	TRENT ET AL.
	Examiner	Art Unit	
	William Bangachon	2635	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>27 December 2005</u>.
2a)☒ This action is **FINAL.**   2b)☐ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-53* is/are pending in the application.
   4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☒ Claim(s) *1-12,23-28 and 35-49* is/are allowed.
6)☒ Claim(s) *13-21,29-32 and 50-53* is/are rejected.
7)☒ Claim(s) *22,33 and 34* is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.
10)☒ The drawing(s) filed on <u>9/21/2000</u> is/are: a)☐ accepted or b)☒ objected to by the Examiner.
   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a)☐ All b)☐ Some * c)☐ None of:
      1.☐ Certified copies of the priority documents have been received.
      2.☐ Certified copies of the priority documents have been received in Application No. _____.
      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
   * See the attached detailed Office action for a list of the certified copies not received.

DETAILED ACTION

Response to Arguments

1.   Applicant's arguments filed 12/27/2005, with respect to amended claims 13-21 and 29-34 have been fully considered but they are not persuasive.

The Examiner respectfully traverses applicant's arguments that Wagener do not disclose a) **"an alarm signal in response to an unauthorized interruption of communication via said port"**. In that Wagener do no disclose the b) **"unauthorized interruption of said communication via said port"** [paragraph bridging pages 27 and 28 - page 32]. The Examiner traverses applicant's arguments that c) **"a breach of a network security loop in Wagener"** is not a convincing evidence of an unauthorized interruption of communication link 30 [page 31, 1st paragraph], d) **"there is no basis nor motivation for to support Examiner's rejection"** [page 32, last paragraph], and that e) **"the proposed combination is nothing more that a hindsight reconstruction of the art provided by the applicant alone"** [page 33, 1st paragraph].

First of all, it is well known to those ordinary skilled in the art that communication between two or more devices can be established in a wired or wireless communication link. Wired communication links between two or more devices comes in different flavors, such as a cable, a twisted pair or optical fiber. For two or more devices to be connected by wired communication links, it is conventional that these cables or twisted pair has connectors at the ends for connecting the two or more devices through their respective ports, for ease of connection and maintenance. Twisted pair type can be

found on most stores, such as radio shack, and would usually have connectors at the ends for connecting two devices at their respective ports. Twisted pair type with connectors used to connect a computer port and a printer port is one example. Twisted pair type with connectors used to attach a monitor to a computer via a computer port would be another example. Networked computers would usually use cables that are protected from noise so that communications between computers cannot be interrupted, such as the cables used to connect a TV to a cable provider, and would use different type of communication port. In a wireless communication link, communication is established between two or more devices via transmit and receive ports. Obviously, any one of the well-known communication links and conventional cables or twisted pairs exemplified above, are suitable for connecting and establishing communication between the protected device and the guard computer of Wagener, to one of ordinary skill in art.

With regards to the disclosure of Wagener, Figure 1 in Wagener shows the communication link 30 (network security loop) connecting the protected electronic device 12 to the guard computer 31 via a port 10. In Figure 2, Wagener shows a more detailed description of the port 10, connected to an outside line via the interface facility 18, such as the network interface, external alarm, and guard computer. Clearly, the communication link 30 is used to transfer data between the protected device 12 and guard computer, such as security data. In the specification, Wagener teaches that **the disconnection of the electronic device 12 from the network security loop triggers an alarm condition** {Wagener, col. 3, lines 45-53}. In another passage of the specification, Wagener teaches that **the breakage or interruption of the protected**

electronic device 12 from the security loop triggers an alarm condition {Wagener, col. 5, lines 45-56}. The **breakage or interruption or disconnection of the protected electronic device 12 from the security loop** (breach of a security loop) would clearly result in a **breakage or interruption or disconnection of the communication** between the protected device 12 and guard computer, because when the communication link 30 between the protected device 12 and the guard computer is disconnected, there are no other means for the protected device 12 to communicate with the guard computer. The **breakage or interruption or disconnection of the communication** between the protected device 12 and guard computer is clearly unauthorized because it triggers an alarm condition {Wagener, Wagener, col. 3, lines 45-53; col. 5, lines 45-56}. Otherwise, there is no reason for triggering an alarm condition if the **breakage or interruption or disconnection** of the protected electronic device 12 from the security loop is not authorized. As exemplified by Wagener, **the protected device is being stolen** {Wagener, col. 7, lines 12-16}. Clearly, the guard computer establishes that the protected device is being stolen if there is a breach of the network security loop, so that the guard computer cannot communicate with the protected device. This breach of the network security loop is an inherent indication of an unauthorized interruption or disconnection of communication in the communication link 30 of Wagener. Otherwise, there is no way for the guard computer to determine whether the protected device is being stolen. Clearly, the unauthorized interruption of communication is via the port 10 or 18, because it is inherently via this port that cable connection is made, as shown in the figures 1 and 2, between the protected device and

guard computer, so that communication is possible between the protected device and the guard computer through the communication link 30 to determine whether the protected device 12 is being stolen. Therefore, **the breakage or interruption or disconnection of the protected device 12 from the security loop** {Wagener, Wagener, col. 3, lines 45-53; col. 5, lines 45-56} is a clear indication of an unauthorized interruption of communication via said port, as claimed, because the guard computer determines that the protected device is being stolen {Wagener, col. 7, lines 12-16} if communication between the protected device is interrupted. In response to the unauthorized disconnection of the communication link between the protected device and guard computer, an alarm condition is triggered.

Wagener teach of numerous examples of such unauthorized interruption of communication that triggers an alarm condition via the port 10, as claimed. Another instance is shown in Figures 5 and 6, wherein Wagener shows a security loop 34a connecting a protected electronic device 12a to an immovable object. Wagener discloses **"an alarm sensor 13a is adapted to detect the detachment of the protected electronic device 12a from the immovable object 36a, so that an alarm is output if the protected electronic device 12a is being stolen"** {Wagener, col. 7, lines 9-16}. Clearly, the unauthorized removal of the protected device 12a detaches the communication link between the protected device and the immovable object and interrupts the communication between the protected device 12a and the immovable object 36a, which in turn, an alarm is output. In other examples, Wagener discloses, **"an alarm condition is generated when a block 44a (a port) is disconnected"**

{Wagener, col. 7, lines 49-53}. Clearly, the unauthorized disconnection of the port (block 44a) would disconnect the communication link and interrupt communication, and in turn, signals the system to generate an alarm condition. And in Figure 7, Wagener shows how a communication link 56b is guarded from an unauthorized interruption of communication via a port 10b, between a protected device 12 and guard computer 31b, that is communicating via a transceiver 54b. These numerous examples by Wagener of an alarm being generated when the protected device is disconnected from the network loop should be ample evidence to show that in the event of theft, the disconnection of the protected device from the network security loop is "an unauthorized interruption of communication of said communication via said port, which generates the alarm condition", as claimed.

Finally, it has been shown that applicant's claimed feature of **"an alarm signal in response to an unauthorized (theft) interruption of communication (the breakage or interruption or disconnection of the protected device 12 from the security loop effectively disconnects or interrupts or disconnects the communication link between the protected device and guard computer) via said port 10 or 18"** is not based upon improper hindsight reasoning or applicant's own disclosure, as argued. But instead, based on Wagener's disclosure as shown {Wagener, Figures 1-7; col. 3, lines 45-53; col. 5, lines 45-56; col. 7, lines 9-16; col. 7, lines 12-16; col. 7, lines 49-53}. It is for these reasons that the rejection of claims 1-12, 23-28 and 35-49 as being unpatentable over the disclosure of Wagener, is maintained in this Final Office action as follows:

2.   Applicant's arguments with respect to new claims 50-53 have been considered

but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

4.   The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148

USPQ 459 (1966), that are applied for establishing a background for determining

obviousness under 35 U.S.C. 103(a) are summarized as follows:

1.   Determining the scope and contents of the prior art.
2.   Ascertaining the differences between the prior art and the claims at issue.
3.   Resolving the level of ordinary skill in the pertinent art.
4.   Considering objective evidence present in the application indicating
       obviousness or nonobviousness.

5.   This application currently names joint inventors. In considering patentability of

the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of

the various claims was commonly owned at the time any inventions covered therein

were made absent any evidence to the contrary. Applicant is advised of the obligation

under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was

not commonly owned at the time a later invention was made in order for the examiner to

consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g)

prior art under 35 U.S.C. 103(a).

6.   Claims 13-21, 29-34 and 50-53 are rejected under 35 U.S.C. 103(a) as being

unpatentable over USP 6,111,505 (Wagener).

In claims 13 and 50-53, a container manager (Fig. 1), comprising:

a housing (12) comprised of a plurality of sidewalls bearing a movable lid,

forming a container having a closed interior while said lid is in complete engagement

with said housing, and providing an open interior able to removably receive items/cargo

within said open interior after movement of said lid is from said complete engagement

{Fig. 1; col. 2, lines 45-57; col. 3, lines 2-21}. In this case, the removable items/cargo

are computer peripherals;

a port (I/O port) mounted to pass data signals through said housing {col. 3, lines

31-35; col. 4, lines 20-26, lines 41-45}. In this case, the I/O port of Wagener allows the

security system of Wagener to be connected to an outside link (30), such as a network

link, telephone link, infra-red link, radio links, cable links, etc. {col. 2, lines 15-25};

a controller (10) comprised of a memory (16) {col. 4, lines 10-19} storing

information specific to said container {col. 3, lines 23-25}, said controller being mounted

entirely within said container, being completely encased by said container during said

complete engagement {col. 3, lines 21-23}, and being operationally coupled to provide

communication by data signals with said interior via said port {col. 3, lines 25-31} and to

operationally respond to data signals received from sources external to said container

{col. 4, lines 27-45} via said port by regulating said movement in dependence upon said information {col. 3, lines 40-45}, and generating an alarm signal in response to an unauthorized interruption of said communication via said port {col. 3, lines 45-50; col. 5, lines 5-8, lines 45-56}; and an alarm (13) {col. 3, lines 54-67} driven by said controller to broadcast an indication of said unauthorized interruption in response to said alarm condition {col. 3, lines 50-53; col. 4, lines 27-45; col. 5, lines 8-12}. Figure 2 shows the communication link 30 is connected to a network interface, external alarm, guard computer (network security loop). The disconnection of the electronic device 12 from the network security loop triggers an alarm condition {Wagener, col. 3, lines 45-53}. The breakage or interruption of the protected electronic device 12 from the security loop triggers an alarm condition {Wagener, col. 5, lines 45-56}. Figures 5 and 6 shows a security loop 34a connecting a protected electronic device 12a to an immovable object. An alarm sensor 13a is adapted to detect the detachment of the protected electronic device 12a from the immovable object 36a so that an alarm is output if the protected electronic device 12a is being stolen {Wagener, col. 7, lines 9-16}. Further, an alarm condition is generated when a block 44a is disconnected {Wagener, col. 7, lines 49-53}. Figure 7 also shows how the communication link 56b is protected via a transceiver 54b. The disconnection or breakage or interruption or detachment of the network security loop in Wagener is clearly an unauthorized interruption of communication, recited in the claim.

Although Wagener do not disclose expressly **"cargo"**, it would have been obvious to one of ordinary skill in the art to have the enclosure of Wagener to contain cargo, such as computer peripherals, to one of ordinary skill in the art.

Claims 14-16 are directed towards different types of communication ports (socket, infrared receiver, antenna). In this case, the I/O port of Wagener allows the security system of Wagener to be connected to an outside link (30), such as a network link, telephone link, infrared link, radio links, cable links, etc. {col. 2, lines 15-25}. Figure 5 shows a cable (38a) used as a communication link. Obviously, the I/O port of Wagener has a socket to connect the cable (38a) to the security system (12a), to one of ordinary skill in the art. And obviously, an infrared communication link would require an infrared receiver, and therefore, would have been obvious in the system of Wagener, to one of ordinary skill in the art. Further, Figure 7 shows a 56b as a communication link. Obviously, the I/O port of Wagener has an antenna to communicate with the transceiver (54b), to one of ordinary skill in the art.

In claim 17, the container manager of claim 13, further comprised of:

a microprocessor based host computer (31) operationally coupled to said controller via said port, generating said data signals; and a data cable (38a) coupling said host computer to said port while conveying said data signals to said controller via said port {col. 5, lines 41-44}.

In claim 18, the container manager of claim 13, further comprised of:

a microprocessor based host computer (31) operationally coupled to said controller via said port, generating said data signals; and a local area network coupling said host computer to said port while conveying said data signals to said controller via said port {col. 2, lines 15-25}.

In claim 19, the container manager of claim 13, further comprised of:

a microprocessor based host computer operationally coupled to said controller via said port, generating said data signals;

said port comprising a first antenna mounted on one of said sidewalls,

a data transceiver connecting said first antenna and said controller; and a second antenna driven by said host computer, operationally connecting said host computer to said first antenna while conveying said data signals to said controller via said first antenna {col. 8, lines 1+}.

In claim 20, the container manager of claim 13, further comprised of:

a microprocessor based host computer operationally coupled to said controller via said port, generating said data signals;

an infrared transmitter driven by said host computer to broadcast an infrared signal corresponding to said data signals; and

an infrared receiver mounted in one of said sidewalls, disposed to receive and convey to said controller said data signals from said infrared transmitter {col. 2, lines 15-25}.

In claim 21, the container manager of claim 13, further comprised of:

a microprocessor based host computer operationally coupled to said controller via said port, generating said data key;

a first infrared transmitter and receiver driven by said host computer to broadcast an infrared signal corresponding to said data key; and

a second infrared transmitter and receiver mounted in one of said sidewalls, disposed to receive said data key from said infrared transmitter, and to transmit operational communications from said controller to said host computer via said first infrared transmitter and receiver {col. 2, lines 15-25}.

Claims 29-31 recites the combination of claims 13 and 19-21, and therefore rejected for the same reasons.

In claim 32, Wagener do not disclose **"a second alarm driven by said host computer"**. However, in a wireless configuration shown in figure 7, Wagener teach of transceivers 54b outputting a signal indicative of an alarm condition (interruption of communication) to the guard/host computer (31b) {col. 8, lines 45-51}. Obviously, the guard computer drives a second alarm for notifying security personnel {col. 8, lines 14-18}, to one of ordinary skill in the art.

Allowable Subject Matter

7.   The allowable claims and reasons for allowance stated below were previously indicated in the last Office action. It is included in this Office action for completeness as follows:

8.   Claims 1-12, 23-28, and 35-49 are allowed.

9.   As allowable subject matter has been indicated, applicant's reply must either comply with all formal requirements or specifically traverse each requirement not complied with. See 37 CFR 1.111(b) and MPEP § 707.07(a).

10.   The following is a statement of reasons for the indication of allowable subject:

With regards to independent claims 1, 23, and 35, the prior art made of record fails to suggest **"a control stage, generating a control signal in dependence upon disposition of said port relative to a source of said data signals, in dependence upon disposition of said container within a scheme for generation of said data signals, and in response to occurrence of a coincidence between a data key received among said data signals via said port and a data sequence obtained by said control stage in dependence upon said information stored within said memory"**. Claims 2-12, 24-28 and 36-49 are allowable for the same reasons.

11.   Claims 22, 33-34 are objected to as being dependent upon rejected base claims

13 and 29, but would be allowable if rewritten in independent form including all of the

limitations of the base claim and any intervening claims. If allowed, this will effectively

make claims 13 and 15-21, and claims 29-32 allowable.

Conclusion

12.   Applicant's amendment necessitated the new ground(s) of rejection presented in

this Office action. Claims 13-21 and 29-34 was amended and new claims 50-53 have

been added but was rejected. Accordingly, **THIS ACTION IS MADE FINAL**. See

MPEP § 706.07(a). However, although this action is made final, applicant is allowed to

cancel all of the rejected claims to place the application in condition for allowance.

Applicant may submit an affidavit to cancel all rejected claims or may request the

Examiner to cancel all of the rejected claims in an Examiner's amendment. See

Examiner contact information below.

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed.

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date

of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Examiner Contact Information

13.   Any inquiry concerning this communication or earlier communications from the Examiner should be directed to William Bangachon whose telephone number is **(571)-272-3065**. The Examiner can normally be reached on 4/4/1010. If the Examiner is unavailable, please leave a message on the Examiner's answering machine with your name and contact number. Whether it is a request to cancel all of the rejected claims or request for interview or a disagreement of Examiner's Office action, the Examiner will respond in due time. If it is a request for interview, you may be requested to fax a proposed claim amendment or arguments to the Examiner's fax number.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, Michael Horabik can be reached on **(571)-272-3068**. The fax phone numbers for the organization where this application or proceeding is assigned is (571) 273-8300 for regular and After Final formal communications. The Examiner's fax number is (571)-273-3065 for informal communications.

Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry of a general nature or relating to the status of this application or

proceeding should be directed to the receptionist whose telephone number is 703-308-

6071.

William Bangachon
Examiner
Art Unit 2635

March 1, 2006